IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

WEBROOT, INC. and OPEN TEXT, INC., **Plaintiffs,** **v.**	
AO KASPERSKY LAB,	**W-22-CV-00243-ADA-DTG (LEAD CASE)**
TREND MICRO, INC.,	**W-22-CV-00239-ADA-DTG**
SOPHOS LTD.,	**W-22-CV-00240-ADA-DTG**
CROWDSTRIKE, INC. AND CROWDSTRIKE HOLDINGS, INC.,	**W-22-CV-00241-ADA-DTG**
FORCEPOINT, LLC, **Defendants.**	**W-22-CV-00342-ADA-DTG**
CROWDSTRIKE, INC., **Counterclaim-Plaintiff,** **v.** **WEBROOT, INC. and OPEN TEXT, INC.,** **Counterclaim-Defendants.**	

CROWDSTRIKE, INC.'S RESPONSIVE CLAIM CONSTRUCTION BRIEF FOR PATENTS ASSERTED BY COUNTERCLAIM

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

TABLE OF EXHIBITS

Ex.	Name
A	Harry Newton, Newton's Telecom Dictionary (22nd ed. 2006)
B	Counterclaim-Plaintiff CrowdStrike, Inc.'s Preliminary Proposed Claim Constructions (February 1, 2023)
C	U.S. Patent 9,043,903 File History Excerpt – October 23, 2014 Final Rejection
D	U.S. Patent 9,043,903 File History Excerpt – January 15, 2015 Amendment
E	Declaration of Dr. C. Jules White
F	Anne Aarness, "What is Endpoint Detection and Response (EDR)?" (Feb. 6, 2023)
G	Marcos Osorno et al., "Coordinated Cybersecurity Incident Handling" (June 2011)
H	Gabriel Klein, "Towards a Model-Based Cyber Defense Situational Awareness Visualization Environment" (October 2010)
I	Excerpted Slides from Plaintiffs Open Text Inc. and Webroot LLC's Claim Construction Presentation re: Plaintiff's [sic] Asserted Patents (Mar. 14, 2023)

I. INTRODUCTION

None of the exceptions permitting a departure from the plain and ordinary meaning apply to the four terms that Counterclaim-Defendants OpenText, Inc. and Webroot, Inc. (collectively, "OTI") seek to construe. OTI has not identified any lexicography, disavowal, or limiting statements justifying such a departure. Indeed, the intrinsic evidence lacks the basis necessary to support OTI's constructions. Further, in many of OTI's constructions, it introduces unnecessary ambiguity by redrafting these terms, including by using language not supported by the intrinsic evidence. Instead, the intrinsic evidence confirms that Counterclaim-Plaintiff CrowdStrike, Inc.'s ("CrowdStrike") patents' use of the claim terms is consistent with their plain and ordinary meanings to a POSITA. Conversely, the only term CrowdStrike seeks to construe ("tracking attributes or behaviors of one or more processes . . .") is necessary to aid the jury and is rooted in the intrinsic evidence. OTI chose not to address this term, thus conceding to CrowdStrike's construction.

II. BACKGROUND OF THE '903 AND '784 PATENTS

U.S. Patent No. 9,043,903 ("the '903 patent") is the parent patent to U.S. Patent No. 9,904,784 ("the '784 patent") (collectively, "Asserted Patents"). The Asserted Patents are directed to a "kernel-level security agent" that is comprised of a model, components, and managers to, among other things, observe, detect, and prevent threats, and communicate with a security service cloud. '903 patent, 1:47-49, 2:21-30, 2:51-60, 3:43-46.[1] In particular, the "kernel-level security agent" does not just observe the events on a computing device, but it also filters and routes those events to other components, such as the "kernel-mode event consumers," to take certain actions. 2:60-64. The Asserted Patents also teach that a communications module of the "kernel-level

[1] Citations to the specification refer to the '903 patent, but those citations apply equally to the '784 patent as they share a common specification.

security agent" can communicate with a remote system, such as the security service cloud, to, among other things, "transmit events, other notifications, and data associated events from the kernel-level security agent 114." 10:63-66.

These teachings address various problems in the state of the art of malware detection, one of which is the reliance on "signature-based and heuristic techniques to detect malware." 1:16-19. The prior art systems also had gaps in malware protection due to the pace at which malware is updated, leaving periods of vulnerability when updating the malware definition, updating the antivirus software itself, or booting the computer. 1:27-29. The "kernel-level security agent" overcomes these problems by "load[ing] before the operating system," including "very early in the boot-time" of the computer, to "observe[] and analyse[] all semantically-interesting events that occur." 5:10-15, 2:51-55. As a result, the claimed "kernel-level security agent significantly reduces the window in which malware can become active and interfere with operation of the host computing device or run unobserved on the host computing device." 2:11-18.

III. DISPUTED TERMS

A. "kernel-level security agent" ('903 patent, claims 21, 22, 25, and 27; '784 patent, claims 1, 6, 15, and 17)

CrowdStrike	OTI
No construction necessary	"software that operates in kernel-mode on a host computing device as a virtual machine/shadow operating system"

No construction is required for this term. Each word within this term is well-known and readily understandable to a POSITA. OTI's construction violates multiple canons of claim construction—each on their own is enough to show that OTI's construction is wrong.

1. The Claim Term And Its Individual Words Are Clear

The claim term "kernel-level security agent" is "not difficult or too technical in nature such that a construction would aid the jury in understanding." *Flypsi, Inc. v. Dialpad, Inc.*, No. 6:21-

CV-00642-ADA, 2022 WL 3593131, at *3 (W.D. Tex. Aug. 22, 2022). For example, the specification discloses that the "kernel-level security agent" "loads before the operating system," including "very early in the boot-time" of the computer, and that it "observes and analyses all semantically-interesting events that occur." 2:7-18, 2:48-55. An exemplary process is described as "implemented by the kernel-level security agent . . . for detecting a first action associated with malicious code, refraining from preventative action while gathering data, and upon detecting subsequent action(s) associated with the malicious code, performing a preventative action." 1:50-55. The specification makes clear what the "kernel-level security agent" is and what it does.

The extrinsic evidence is consistent with the intrinsic evidence. For example, a 2006 dictionary defined "kernel" to be "the level of an operating system or networking system that contains the system-level commands or all of the functions hidden from the user." Ex. A at 23909. "Agent" is also a term with a "well-established meaning" in the context of the specification. *Ancora Techs., Inc. v. LG Elecs. Inc.*, No. 1:20-CV-00034-ADA, 2020 WL 4825716, at *19 (W.D. Tex. Aug. 19, 2020). And OTI does not dispute that the term "security" is commonplace in the context of computers. All "the components of the term [kernel-level security agent] have well-recognized meanings," so a POSITA can "infer the meaning of the entire phrase with reasonable confidence." *Bancorp Services, L.L.C. v. Hartford Life Ins. Co.*, 359 F.3d 1367, 1372 (Fed. Cir. 2004).

2. OTI's Proposed Construction Improperly Reads Limitations From The Specification Into The Claims

First, the specification does not limit a "kernel-level security agent" to just "a virtual machine/shadow operating system." The specification that OTI relies on simply informs the POSITA that the "kernel-level security agent" functions "***as*** a virtual machine/shadow operating system"—in other words, ***like*** "a virtual machine/shadow operating system"—but does not say it

is limited to just a "virtual machine/shadow operating system." 2:4-7, 5:9-10. The specification supports CrowdStrike's position, as it indicates that only "***some*** implementations . . . of the computing device 102 . . . represents one or more virtual machines." 4:34-38.[2] OTI's inclusion of "as a virtual machine/shadow operating system" is problematic because it requires "constru[ing] [a] term functionally—*i.e.*, by its intended result," not by what the "kernel-level security agent" is. *Medicines Co. v. Mylan, Inc.*, 853 F.3d 1296, 1306 (Fed. Cir. 2017).

Second, OTI's construction improperly narrows "kernel-level" by replacing it with "operates in kernel-mode." The specification never uses the phrase "operates in kernel-mode." It also never limits the "kernel-level security agent" to just operating in the kernel-mode, *i.e.*, one of two states in which a computer may operate (the other being user mode). Instead, the specification provides examples of where a "kernel-level security agent" can operate, such as "a kernel-level security agent that ***operates on a host computing device***" (2:4-7) or "[t]he kernel-level security agent 114 ***operates as a virtual machine/shadow operating system***" (5:9-10).

While certain modules of the "kernel-level security agent" may be implemented at the "kernel-level," not all modules of the "kernel-level security agent" must be implemented or even operated at that level. For example, claim 2 recites that "the kernel-level security agent include[s] a collector component configured to observe kernel-level or ***user-level events*** and to provide at least a subset of the observed events to the configurable filters," which makes clear that the "kernel-level security agent" is observing events even outside of kernel-mode. Claim 2. Further, claim 21 states that the "communications module" is "implemented at the kernel-level," while the specification and claim 2 teaches that other aspects of the "kernel-level security agent," such as the claimed "configurable filters," can be implemented at "user mode." 8:37-50; *see also* 7:56-

[2] All emphasis herein are added by CrowdStrike unless otherwise noted.

8:14, 10:55-11:4, claims 2, 21. The specification explicitly defines how certain components, such as the "configurable filters 210" of the "kernel-level security agent," may be "user mode components":

> As mentioned, the security agent architecture may further include configurable filters 210. ***The configurable filters 210 may be user mode components 116 of the kernel-level security agent*** 114 that filter user mode events observed by the user mode collectors 208 based on the configuration of the kernel-level security agent 114.

8:37-42. This is further shown in Figure 2, which illustrates an example "kernel-level security agent" and shows **components 116** in **kernel-mode** and **user mode**:

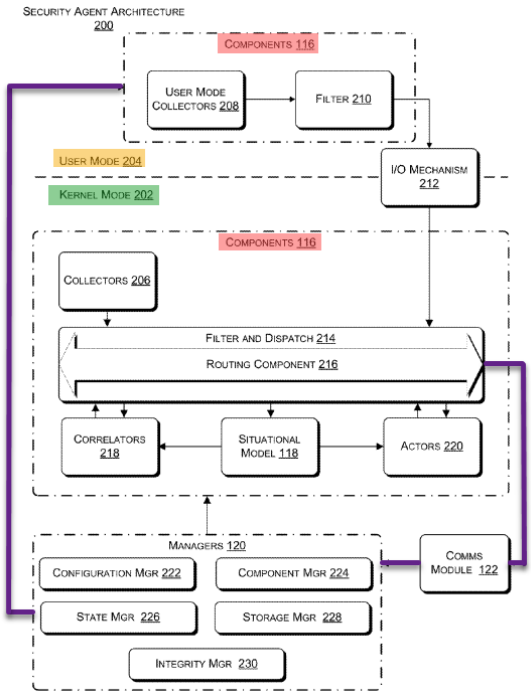

Fig. 2. As a result, there is no requirement in the specification that a "kernel-level security agent" operate entirely in "kernel-mode." OTI's construction again improperly reads out those embodiments.[3] *In re Katz Interactive Call Processing Patent Litig.*, 639 F.3d 1303, 1324 (Fed.

[3] OTI itself recognized at the March 14 *Markman* hearing that "a user mode function can transition to the kernel mode," which undercuts its own proposed construction here that something at "kernel-level" must operate solely in kernel-mode. Dkt. 147 at 25-26.

Cir. 2011) ("[T]here is a strong presumption against a claim construction that excludes a disclosed embodiment.").

OTI's inclusion of "kernel-mode" also violates canons of claim differentiation. Both "kernel-mode" and "kernel-level" are used as two different terms in the claims. Claim 21 requires "the filtered events to one or more ***kernel-mode*** event consumers of the ***kernel-level*** security agent." Claim 21. The claims require that the "event consumers" be in "kernel-mode" but do not require that all aspects of the "kernel-level security agent" be in "kernel-mode." *Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) (finding the doctrine of claim differentiation violated when a proposed construction renders another claim "superfluous and redundant").

Third, OTI's proposed construction reads out the word "security" from "kernel-level security agent." Indeed, none of the words in OTI's proposed construction are substantially similar to the term "security." Given that the Court "must give meaning to all the words in [the] claims," OTI's proposed construction cannot be correct. *Exxon Chemical Patents, Inc. v. Lubrizol Corp*., 64 F.3d 1553, 1557, (Fed. Cir. 1995); *Fran Nooren Afdichtingssystemen B.V. v. Stopaq Amcorr Inc.*, 744 F.3d 715, 722 (Fed. Cir. 2014) ("the construction of a clause as a whole requires construction of the parts, with meaning to be given to each part . . . .").

All of OTI's cases are distinguishable, as the allegedly "limiting" statement OTI primarily relies on does ***not*** (1) include the phrase "present invention;" (2) appear in the Abstract or Summary of the Invention of the Asserted Patents; or (3) appear as OTI's proposed construction in every embodiment. *C.R. Bard, Inc. v. U.S. Surgical Corp*., 388 F. 3d 858, 864 (Fed. Cir. 2004); *Verizon Servs. Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1308 (Fed. Cir. 2007); *Microsoft Corp. v. Multi-Tech Sys*., *Inc*., 357 F.3d 1340, 1348 (Fed. Cir. 2004); *Retractable Techs. Inc. v.*

Becton, Dickinson and Co., 653 F.3d 1296, 1305 (Fed. Cir. 2011). Even the disclosure in the "Detailed Description" section is "not wholly dispositive" because as discussed herein, there are additional, compelling reasons to deny OTI's proposed construction. *MBO Lab'ys, Inc. v. Becton, Dickinson & Co.*, 474 F.3d 1323, 1330 (Fed. Cir. 2007).

3. OTI Added Or Replaced Words That Are Unsupported

OTI's construction adds the phrase "***host*** computing device." But claim 21 already requires "observing, by a kernel-level security agent, events on ***a computing device***" and does not require the "computing device" to be a "host." Claim 21. The specification uses both "host computing device" (*see, e.g.*, 2:4-5) and "computing device" (*see, e.g.*, 3:52-62), and likewise does not dictate that a "computing device" be a "host computing device."[4] %

OTI's proposed construction unnecessarily replaces "agent" with "software," which is improperly broader. As discussed above, the term "agent" also has a "well-established meaning." *Ancora*, 2020 WL 4825716, at *19; Br., Ex. 4 at -907-08. Thus, the Court should decline to "replace[] [an] easily understandable word with a potentially confusing phrase intended to express the same meaning." *Phoenix Licensing, L.L.C. v. AAA Life Ins. Co.*, No. 2:13-CV-1081, 2015 WL 1813456, at *28 (E.D. Tex. Apr. 20, 2015).

B. "kernel-mode event consumers" ('903 patent, claims 21, 25, and 27; '784 patent, claim 15)

CrowdStrike	OTI
No construction necessary	"event consumers operating in kernel mode"

OTI contends that its construction is necessary based on an alleged disclaimer of claim scope during prosecution. Br. at 6-7. But disavowal of claim scope is a very high bar to prove, and

[4] If OTI's construction is adopted, the claim language would be more confusing, as it would require one "host computing device" for the claimed "kernel-level security agent" and another "computing device" for the observed events, which is contrary to the teachings of the specification that require the "kernel-level security agent" to observe events on the endpoint that it resides on.

OTI has failed to show the clear, "exacting" standard needed to demonstrate that the Applicants limited "kernel-mode event consumers" during prosecution. *Intell. Ventures I LLC v. T-Mobile USA, Inc.*, 902 F.3d 1372, 1378 (Fed. Cir. 2018); *Cordis Corp. v. Boston Scientific Corp.,* 561 F.3d 1319, 1329 (Fed. Cir. 2009) ("A disclaimer must be 'clear and unmistakable'").

To support its alleged prosecution history disclaimer, OTI contends the Applicants amended their claims and also stated that this amendment was intended "[t]o make clear that the claimed 'one or more event consumers' operate in kernel-mode" to overcome the Examiner's prior art rejection to Costea. Br. at 6. But OTI's proposed construction is unnecessary, as the very purpose of the Applicants' amendment in the first place was to clarify that the claimed "one or more event consumers" are in kernel-mode; that is why they amended "event consumers":

> For example, the "one or more event consumers" of claim 1 are described in the present application as correlators or actors (paragraph 12) and, as shown in figure 2 of the present application, correlators and actors are kernel-mode components of the kernel-level security agent. ***To make clear that the claimed "one or more event consumers" operate in kernel-mode, Applicant herein amends claim 1 to recite that the events consumers are "one or more kernel-mode event consumers."***
>
> In Costea, in contrast, the only components which "take action based at least on one of the filtered events" are the user-mode security service application and antivirus software. The only kernel-mode component in Costea, the generalized security filter, simply record file system operations in a section object. ***Thus, Costea does not disclose, expressly or inherently, "one or more kernel-mode event consumers to take action based at least on one of the filtered events," as is claimed in amended claim 1***.

Br., Ex. 5 at 15. This was not a disclaimer, but a clarification of claim scope that is already baked into the claim term itself. The Examiner also agreed that the Applicants' amendment was sufficient. Since the claim term here already includes "kernel-mode" in front of "event consumer," there is no need to construe this claim term as OTI suggests.

C. "the communications module being implemented at the kernel-level" ('903 patent, claim 21)

CrowdStrike	OTI

No construction necessary	"the communications module operating in kernel-mode"

Just as with "kernel-level security agent," OTI's construction improperly changes "implemented at the kernel-level" to "operating in kernel-mode." *See supra*, § III.A.2. A module that is implemented at the kernel-level is not merely restricted to only operating in kernel-mode, as the module may give instructions or otherwise control other modules in user-mode. *Id.*

OTI couches its construction as a clarification. Br. at 8. It contends that "being implemented" is "ambiguous," because it could mean "operating in user mode or referring to something that does not involve computer operations."[5] *Id*. But OTI's construction improperly limits the scope of this term from that set forth in the intrinsic evidence. Nowhere in the intrinsic evidence does it use the word "operating in kernel-mode" to describe the "communications module." And for good reason, because doing so would preclude the "communications module" from its very purpose, which is to communicate with user-level modules in the same or remote computers.

The specification discloses that the communications module 122 is a component of the kernel-level security agent 114, as shown in Figure 1 and "may, as illustrated in Fig. 2, be a kernel-mode component of the computing device 102." 10:61-63. Further, the specification states that the communications module 122 can "***communicate with the security service cloud 104***," which may involve transmission of "events, other notification, and data associated events from the kernel-level security agent 114 to the security service cloud 104." 10:61-66. The specification further describes that the communications module 122 may "transmit configuration updates ***received from the security service cloud 104*** to a configuration manager 222 of the kernel-level security agent

[5] CrowdStrike does not address OTI's latter basis for ambiguity, as any reasonable POSITA or jury would not consider the term "implemented" in the context of the intrinsic evidence to be expanded in such manner to "not involve computer operations."

114 and healing instructions and/or events from the security service cloud 104 to an actor 220." 10:66-11:4. This shows that in certain embodiments, the communications module may be implemented at the kernel-level, but that the communications module can still communicate with modules that are outside of the kernel-level, such as the security service cloud 104 and other modules of the kernel-level security agent 114 that are user-level.

OTI's cited passages from the specification do not support OTI's construction. At 7:36-38, the '903 patent merely confirms that the "communications module 122" is a part of the "kernel-level security agent 114," which, as discussed above, includes user-mode components. *See supra*, § III.A.2. A description of Figure 2 that the "communications module 122 ***may*** . . . be a kernel-mode component" does not justify limiting the operations of the communications module 122 to just kernel-mode and preventing it from communicating with components in user mode.[6] 10:61-63. By replacing "implementing" with "operating," OTI wants to preclude the "communications module" from having any interaction with the user-level, including communicating, which is not correct and contradicts the intrinsic evidence.

OTI's reliance on the prosecution history is also misplaced and does not limit the "communications module" to "operating in kernel-mode." Br. at 10-11. There, the Applicants noted that ***the Examiner*** held that that the generalized security filter in Costea is the "communications module implemented at the kernel-level." Br., Ex. 5 at 16. The Applicants, however, disagreed with the Examiner and stated the following:

> Applicant respectfully submits that Costea does not describe any such communication module. While Costea does describe a generalized security filter implemented in kernel-mode, that generalized security filter does not "communicate with one or more remote systems."

[6] OTI's argument that "[n]owhere in the specification is the communications described as being in user mode" (Br. at 9) is belied by the recited passages above and does not otherwise justify OTI's unsupported limitation.

Id. The Applicants distinguished Costea's generalized security filter on the basis that it did not "communicate with one or more remote systems," not that the entirety of the claimed communications module must operate solely in kernel-mode. *Id*. This distinction over Costea is already captured by the language in claim 21, which requires "communicating, by a communications module of the kernel-level security agent, ***with one or more remote systems***." Claim 21. And Costea actually supports the plain and ordinary meaning of this claim term, as it discloses that the generalized security filter 316 "intercepts I/O requests made from user applications" and "communicates with the security service application 314," which is shown in Figure 3 to be in user-mode. Br., Ex. 6 at 6:34-48.

None of the intrinsic evidence supports OTI's proposed construction, which improperly removes the very purpose of the "communications module" from the claims.

D. "tracking attributes or behaviors of one or more objects or processes of the system in a model of the kernel-level security agent" ('903 patent, claim 22)

CrowdStrike	OTI
"tracking attributes or behaviors of one or more objects or processes of the computing device in a model of the kernel-level security agent"	Indefinite

As an initial matter, OTI did not brief this term in their Opening Brief despite CrowdStrike identifying this term for construction and providing OTI with CrowdStrike's construction for this term. Ex. B at 2. Thus, OTI has waived argument on this term and cannot raise new arguments for the first time on reply.[7]

The intrinsic evidence supports CrowdStrike's construction that "the system" of dependent

[7] *Novosteel SA v. U.S., Bethlehem Steel Corp.*, 284 F.3d 1261, 1274 (Fed. Cir. 2002) ("Raising the issue for the first time in a reply brief does not suffice[.] . . . As a matter of litigation fairness and procedure, then, we must treat this argument as waived."); *Docusign, Inc. v. Sertifi, Inc*., 468 F. Supp. 2d 1305, 1307 (W.D. Wash. 2006) (finding that new arguments regarding claim construction are inappropriate for reply and waived.). OTI agreed that arguments raised on reply for the first time are waived in their responsive claim construction brief on OTI's first wave of patents. Dkt. 98 at 6-7.

claim 22 is the "computing device" of independent claim 21 (from which claim 22 depends). The claims, specification, and file history confirm that the claimed "tracking attributes or behaviors of one or more objects or processes" in claim 22 is of "the computer device" of claim 21 and not of the "remote systems" of claim 21. CrowdStrike seeks construction of this term to minimize jury confusion as to what "the system" in claim 22 refers to in connection with claim 21.

Looking first at the claims, claim 21 is directed to a method for observing "events on a computer device" and then performing certain actions by a "kernel-level security agent" based on those events observed. The "kernel-level security agent" communicates with "remote systems" to, for example, inform "remote systems" of certain information about the observed events. Claims 21, 23. While claim 21 explains that information about the events is communicated to the "remote systems," the events themselves are from the "computing device" and the observations and steps taken by the "kernel-level security agent" are all based on those events on the computer device. Claim 22 sets forth further steps taken by the "kernel-level security agent" of claim 21—it claims "tracking attributes or behaviors of one or more objects or processes." Claim 22 states that the "objects or processes" is "of the system," but it is clear that "of the system" refers to the claimed "computing device" of claim 21, since the "kernel-level security agent" resides ***on the computing device*** and takes no actions on any remote systems.

The specification consistently explains that the "kernel-level security agent" is responsible for "track[ing] attributes and behaviors of processes ***of the computing device***":

> The situation model represents chains of execution activities and genealogies of processes, ***tracking attributes, behaviors, or patterns of processes executing on the host computing device*** and enabling an event consumer of the kernel-level security agent to determine when an event is interesting

3:1-6.

> The kernel-level security agent 114 may include components 116 to observe events and determine actions to take based on those events, a situational model 118 to

> ***track attributes and behaviors of processes of the computing device*** 102, managers 120 to update the components 116 and provide continual detection during updates, and a communications module 122 to communicate with the security service cloud 104.

3:62-4:2.

> In further embodiments, the situation model 118 of the kernel-level security agent 114 may comprise any one or more databases, files, tables, or other structures that ***track attributes, behaviors, and/or patterns of objects or processes of the computing device*** 102.

9:60-64; *see also* 10:26-35. The specification never refers to the "kernel-level security agent" tracking attributes or behavior of objects of a "remote system"; it is always of a "computing device." *Wisc. Alumni Res. Found. v. Apple Inc.*, 905 F.3d 1341, 1350-52 (Fed. Cir. 2018) (claim term "prediction" required to receive updates as it was repeatedly and consistently referred to in the specification as being able to receive updates and the specification did not describe any other embodiments).

The file history provides context for how "the system" ended up in claim 22, and how the claimed "tracking [of] attributes or behaviors of one or more objects or processes" is of "the computing device" and cannot be of the "remote devices" of claim 21. In a July 7, 2014 amendment, the Applicants added claims 34 and 35 in the then-pending application, which eventually resulted into issued claims 21 and 22 in the '903 patent:

> 34. (New) A computer-implemented method comprising:
>
> observing, by a kernel-level security agent, events on a computing device;
>
> filtering, by the kernel-level security agent, the observed events using configurable filters;
>
> routing, by the kernel-level security agent, the filtered events to one or more kernel-mode event consumers of the kernel-level security agent; and
>
> taking action, by the one or more kernel-mode event consumers of the kernel-level security agent, based at least on one of the filtered events.
>
> 35. (New) The computer-implemented method of claim 34, further comprising tracking attributes or behaviors of one or more objects or processes of the system in a model of the kernel-level security agent and updating the model based at least in part on the filtered events.

Br., Ex. 5 at 7-8. Claim 34, at the time, did not claim any "remote systems." *Id*. In drafting claim 35, the Applicants converted dependent *system* claim 3 into new dependent method claim 35, which is shown by a simple comparison of the two claims:

Then-dependent system claim 3	Then-dependent method claim 35
3. (Original) The system of claim 1, wherein the kernel-level security agent comprises a model to track attributes or behaviors of one or more objects or processes of the system, and the kernel-level security agent is further configured to update the model based at least in part on the filtered events.	35. (New) The computer-implemented method of claim 34, further comprising tracking attributes or behaviors of one or more objects or processes of the system in a model of the kernel-level security agent and updating the model based at least in part on the filtered events.

Br., Ex. 5 at 2, 8. But in doing so, the Applicants did not remove the reference to "the system" of claim 3. It is clear, however, that "the system" does not refer to the "remote systems," because the "remote systems" was not even a limitation in then-pending independent claim 34 (from which claim 35 depends). And instead, "the system" must refer to the "computing device," which was a limitation in the then-pending claim 34. Br., Ex. 5 at 7-8.

This is made even more clear in subsequent amendments. In an October 23, 2014 Final Rejection, the Examiner rejected all the pending claims, but stated that then-pending dependent claim 5 was allowable if rewritten in independent form including all the limitations of the base claim and any intervening claim. Ex. C at 12. Then-pending claim 5 was the following:

> 5. (Original) The system of claim 1, wherein the kernel-level security agent comprises a communications module implemented at the kernel-level and configured to communicate with one or more remote systems.

Br., Ex. 5 at 3. The Applicants then amended the claims to add the limitation in claim 5 to the independent claims, including to then-pending claim 34, which now claimed "remote systems." Ex. D at 7-8. Based on timing, "the system" of claim 35 could not refer to the "remote systems" of claim 34.

E. "model" ('903 patent, claims 22 and 27; '784 patent claim 9) / "situational model" ('784 patent, claims 1, 2, 3, 12, and 20)

CrowdStrike	OTI
No construction necessary	Indefinite

The claim terms "model" and "situational model" are terms of art that are readily understandable in light of the intrinsic and extrinsic evidence and a POSITA would have no issues determining with reasonable certainty the boundaries of the scope of these claim terms. OTI does not dispute that "model" and "situational model" are described throughout the specification. Br. at 11-13 (quoting pages of specification that describe these terms). Instead, OTI complains that the specification provides too many examples of what could be a "model" or "situational model," and on that basis it alleges these terms are unbound and indefinite. Not so.

The specification describes these claim terms, as it explains that "the situation[al] model 118 of the kernel-level security agent 114 may comprise any one or more databases, files, tables, or other structures that track attributes, behaviors, and/or patterns of objects or processes of the computing device 102." 9:60-64. The specification provides further details on the "attributes, behavior, and/or patterns," explaining that they "may represent execution activities of processes" such that "the situational model 118 may represent chains of execution activities providing genealogies of processes." 9:64-67. As a result, the specification teaches that a "situational model 118," which is referred to as "the model," "stores attributes, behaviors, and/or patterns of events, specific events, and forensic data associated with events." 9:67-10:3 (further explaining that the "data stored by the situational model 118 may be indexed by specific events or by specific types of events"). Figure 2 (reproduced below) illustrates the **situational model 118** in the security agent architecture 200:

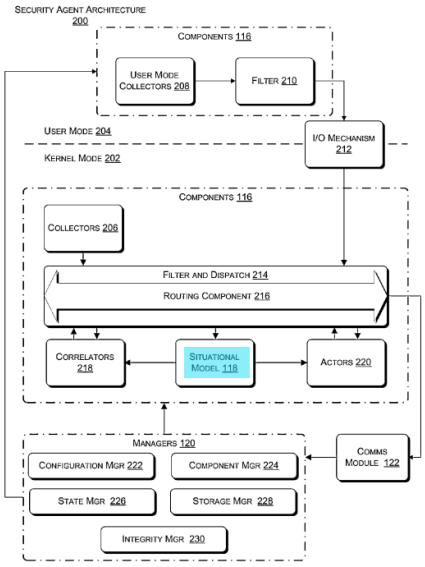

Fig. 2. As shown above and described in the specification, a POSITA would readily understand that the situational model 118 can update its stored information in its data structures by receiving filtered events from the routing component 216 or "forensic data that is associated with events and retrieved by the actors 220," but also "respond[s] to queries from configurable filters 214, correlators 218, or actors 220 with descriptions of attributes, behaviors, and/or patterns of events or with descriptions of specific events. 10:5-15, Fig. 2. This enables the "kernel-level security agent" to continue to accurately determine whether an "event is interesting in some fashion and/or may be associated with malicious code." 10:31-35.

The extrinsic evidence also demonstrates that "model" and "situational model" are commonly understood terms of art that a POSITA would readily understand. Ex. E, ¶ 33. CrowdStrike's description of "model" on its webpage is consistent with the specification.[8] One cybersecurity article published in June 2011 specifically referred to "situational awareness process models" and confirmed their "prevalence . . . in contemporary literature" by "survey[ing] multiple

[8] "The model keeps track of all the relationships and contacts between each endpoint event using a massive, powerful graph database, which provides details and context rapidly and at scale, for both historical and real-time data." Ex. F at 2; Ex. E, ¶ 36.

. . . situational awareness models for their potential application to coordinated incident handling." Ex. G at 1, 2; Ex. E, ¶ 37. In October 2010, another article discussed the need for "[a] model supporting situation awareness with regard to cyber defense" so that "[t]he current situation can then be derived from a known initial situation combined with information about situation changes that happened over time." Ex. H at 1-3; Ex. E, ¶ 37. Both the intrinsic and extrinsic evidence demonstrate that these claim terms are terms of art, and a POSITA would readily understand the scope of these terms with reasonable certainty.

OTI has not met its burden of proving by clear and convincing evidence that the claim terms "model" and "situational model" are indefinite based on the use of terms such as "may comprise," "may represent," or "other." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 898–99 (2014); *Cox Commc'ns, Inc. v. Sprint Commc'n Co. LP*, 838 F.3d 1224, 1231-32 (Fed. Cir. 2016). Even with the use of terms like "may comprise," "may represent," or "other," the specification describes these claim terms in a fulsome, detailed manner with "a general guideline and examples" that would readily apprise a POSITA as to what a "situational model" is and what it does. *Enzo Biochem, Inc. v. Applera Corp.*, 599 F.3d 1325, 1335 (Fed. Cir. 2010).

None of OTI's cited passages prevent a POSITA from determining the boundaries of these claim terms with reasonable certainty. For example, OTI cites to three passages that use the phrases "may comprise" or "may represents" and claims that such use "greatly expands the provided definition." Br. at 14. That is not correct. In describing that the situational model "may comprise any one or more databases, files, tables, or other structures that track attributes, behaviors, and/or patterns of objects or processes of the computing device 102," the Applicants provided additional details as to exemplary types of data structures that the claimed "situational model" could be, clarifying how the tracked information is stored and retained. 9:60-64. As for the passage that

"[t]hese attributes, behaviors, and/or patterns may represent execution activities of process," the Applicants provided further information as to what the "attributes, behaviors, and/or patterns" identified in the definition of these terms can be, which provides more, not less, clarity as to the types of information stored in the aforementioned data structures. 9:64-67. And for the passage "the situational model 118 may represent chains of execution activities providing genealogies of processes," the Applicants again sought to further inform a POSITA as to what is a "situational model" within the context of this patent even though it is a term of art. *Id*. Mr. Schnell's statement that a POSITA "would have been uncertain as to what the scope of [the claims terms] is at least with respect to ***activities***" rings hollow, given that the specification has already provided examples of such activities, *i.e.*, "attributes, behaviors, and/or patterns of objects of the computing device 102." Br., Ex. 3, ¶ 62; 9:60-67; *Bracco Diagnostics Inc. v. Maia Pharms., Inc.*, 839 F. App'x 479, 491 (Fed. Cir. 2020) ("[T]he plain and ordinary meaning of 'may' within the context of this specification is properly understood as indicating an inherent measure of likelihood or possibility. It is not used by a person of skill to describe an event that has no likelihood of occurring.").

OTI also points to use of the word "other" as leaving these claim terms open-ended, which fails for similar reasons. Br. at 14. For "other structures," OTI omits that the immediately preceding list of exemplary structures, such as "databases, files, [and] tables," that provide clarity as to the types of data structures that the "situational model" uses to store the information it tracks. 9:60-64. Contrary to Mr. Schnell's contention, this is not an "open-ended structure list" where the specification "provide[s] no guidance as to what 'other structures' track the attributes, behaviors, or patterns of processes being executed beyond databases, file[s], and tables." Br., Ex. 3, ¶ 63. For "other descriptions associated with the event," OTI likewise omits the immediately preceding list of exemplary descriptions of events, such as "attributes, behaviors, and/or patterns," which as

discussed above, are further described as representing "execution activities of processes." 10:26-35, 9:64-67. Mr. Schnell bases his opinion that a POSITA would not be able to discern the boundaries of this term based on two different parts of the specification describing "attributes, behaviors and patterns"—one with the phrase "other descriptions" and one without—and claims the passage with the phrase "other descriptions" leaves the passage without the phrase "open-ended." Br., Ex. 3, ¶ 63. Again, the examples "attributes, behaviors, and/or patterns" themselves inform the POSITA what the "other descriptions" can be and the lack of the phrase "other descriptions" in one explanation does not render it indefinite. *Niazi Licensing Corp. v. St. Jude Med. S.C., Inc.*, 30 F.4th 1339, 1349 (Fed. Cir. 2022) (finding that written description of "numerous examples" of "an exemplary material" sufficient for definiteness).

OTI relies heavily on *IQASR*—a non-precedential case—which is easily distinguishable. Br. at 12, 15. In *IQASR*, the patentee argued that the term at issue "magnetic fuzz" was "a type of magnetic 'low susceptance microparticle' and also 'magnetically active disassociated microparticles.'" *IQASR LLC v. Wendt Corp.*, 825 F. App'x 900, 905 (Fed. Cir. 2020). The specification further described that "low susceptance microparticles ***could be*** magnetic fuzz," but also "***may be*** magnetically active dissociated particles . . . [which is] not limited to magnetic fuzz." *Id.* Then, the specification confusingly explained that "[d]isassociated magnetically active microparticles ***may be*** magnetic fuzz because these particles ***may be difficult to substantially identify***." *Id.* Ultimately, the Federal Circuit found that for a POSITA to understand what "magnetic fuzz" meant, he or she would have to "find the low susceptance microparticles, and then identify which low susceptance microparticles are disassociated magnetically active microparticles" before dealing with the subjective definition of "difficult to substantially identify," which is not explained in the specification. *Id.* at 905-07. Because a POSITA would have to "wade

through a morass of uncertainty and contradiction," the Federal Circuit found the term "magnetic fuzz" to be indefinite. *Id.* at 905.

In contrast, "model" and "situational model" are fully described in the specification that would readily apprise a POSITA of the scope of these claim terms with reasonable certainty. The passages in the specification that do include the modal verb or non-limiting language merely provide further clarity as to what other data structures or information would be tracked and stored, as discussed above. *See supra*, § III.E. Unlike in *IQASR*, which OTI itself distinguished by arguing that the term "magnetic fuzz" was "a coined term defined ***only*** by non-limiting examples" (Ex. I at 85 (emphasis in original); Br. at 12), the claim terms here are not coined terms and are further informed by a general guideline and examples in the specification that inform a POSITA as to the scope of the terms "model" and "situational model" with reasonable certainty.[9]

OTI has not met its burden by clear and convincing evidence that the claim terms "model" and "situational model" are indefinite, and thus, no construction is necessary.[10]

[9] None of OTI's other cases are applicable. Unlike *Icon Health & Fitness, Inc. v. Polar Electro Oy*, CrowdStrike is not relying on another claim term that is "a moving target that may change over time" to delineate the meaning of "model" or "situational model." 656 F. App'x 1008, 1016 (Fed. Cir. 2016). Nor is OTI contending that these claim terms are terms of degree that CrowdStrike has failed to either distinguish from the prior art, like in *Halliburton Energy Servs., Inc. v. M-I LLC*, 514 F.3d 1244, 1253 (Fed. Cir. 2008) (finding term "fragile gel" to be indefinite), or provide "an objective standard to measure against." *CA, Inc. v. Netflix, Inc.*, No. 2:21-CV-00080-JRG-RSP, 2021 WL 5323413, *15-17 (E.D. Tex. Nov. 16, 2021) (finding the term "minimize" to be indefinite).

[10] OTI's arguments here are similar to Sophos' claim construction arguments that it opposed. Sophos cited to the *IQASR* case and latched onto the use of the modal verb "may" as non-limiting examples in the specification. Dkt. 86 at 26-30 (pointing statements in the specification containing the phrase "may comprise"); Dkt. 110 at 14-16. In response, OTI identified examples from the same paragraph relied upon by Sophos that inform the objective boundaries of the disputed term there, including the same non-limiting language it now faults CrowdStrike for here. Dkt. 98 at 32-33; Dkt. 147 at 14-16. Since the Court found that the term "global perspective" should be afforded its plain and ordinary meaning (Dkt. 236 at 8)), the Court should find the same here.

Dated: March 16, 2023

Respectfully submitted,

s/Steven Callahan

DAVID NELSON
QUINN EMANUEL URQUHART & SULLIVAN, LLP
191 N Upper Wacker Dr #2700
Chicago, IL 60606
Tel.: (312) 705-7400
Fax: (312) 705-7401

VICTORIA F. MAROULIS
QUINN EMANUEL URQUHART & SULLIVAN, LLP
555 Twin Dolphin Dr., 5th Floor
Redwood Shores, CA 94065
Tel.: (650) 801-5000
Fax: (650) 801-5100

DEEPA ACHARYA
QUINN EMANUEL URQUHART & SULLIVAN, LLP
1300 I Street, NW, Suite 900
Washington, D.C. 20005
Tel.: (202) 538-8000
Fax: (202) 538-8100

STEVEN CALLAHAN
Texas State Bar No. 24053122
scallahan@ccrglaw.com
CHARHON CALLAHAN ROBSON & GARZA, PLLC
3333 Lee Parkway, Suite 460
Dallas, Texas 75219
Tel.: (214) 521-6400
Fax: (214) 764-8392

Counsel for Defendants CrowdStrike, Inc. and CrowdStrike Holdings, Inc.

CERTIFICATE OF SERVICE

A true and correct copy of the foregoing instrument was served or delivered electronically via U.S. District Court [LIVE]- Document Filing System, to all counsel of record, on March 16, 2023.

s/Steven Callahan
Steven Callahan